PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-258985
(43)Date of publication of application : 24.09.1999

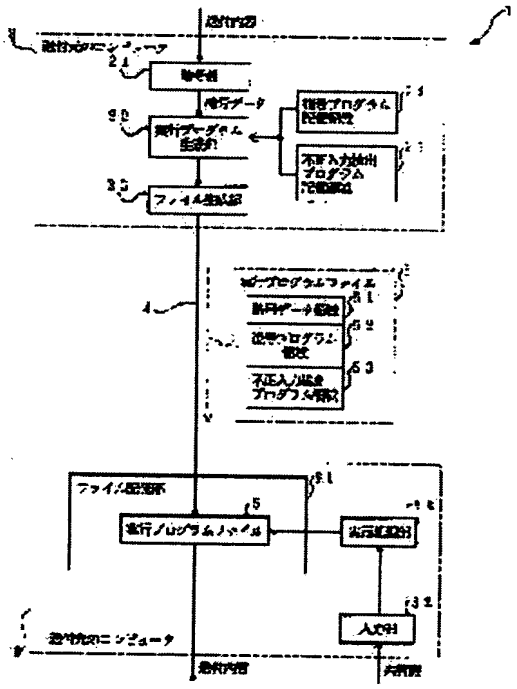
(51)Int.CI. G09C 1/00
G09C 1/00
G06F 9/06

(21)Application number : 10-061626
(22)Date of filing : 12.03.1998

(71)Applicant : NISSIN ELECTRIC CO LTD
(72)Inventor : NAKABAYASHI KIYOHIRO

(54) FILE GENERATING DEVICE FOR SENDING CIPHER DATA, RECORDING MEDIUM WHERE PROGRAM THEREOF IS RECORDED, AND STORAGE MEDIUM STORING FILE FOR SENDING CIPHER DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the cipher data transmission system which is not limited to a transmission destination and can send cipher data safely.
SOLUTION: Relating to a computer 2 at a transmission source, an execution program generation part 22 generates an execution program including cipher data showing transmission contents and a deciphering program. The execution program is sent out to a computer 3 at a transmission destination as an execution program file 5 which can be executed by the computer 3. The computer 3 instructs execution of the execution program file 5 and the said deciphering program deciphers the cipher data once a correct common key is inputted. The execution program 5 is in the same format as execution programs for other purposes of use, so it can be sent more safely than when the cipher data themselves are transmitted. Further, the deciphering program is included in the execution program file 5, so the transmission contents can be sent without preparing the deciphering program on the computer 3.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－258985

(43)公開日　平成11年(1999)９月24日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ｂ
		６６０			６６０Ｄ
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ａ

審査請求　未請求　請求項の数６　ＯＬ　（全 13 頁）

(21)出願番号　特願平10－61626

(22)出願日　平成10年(1998)３月12日

(71)出願人　000003942
日新電機株式会社
京都府京都市右京区梅津高畝町47番地

(72)発明者　中林　聖裕
京都府京都市右京区梅津高畝町47番地　日新電機株式会社内

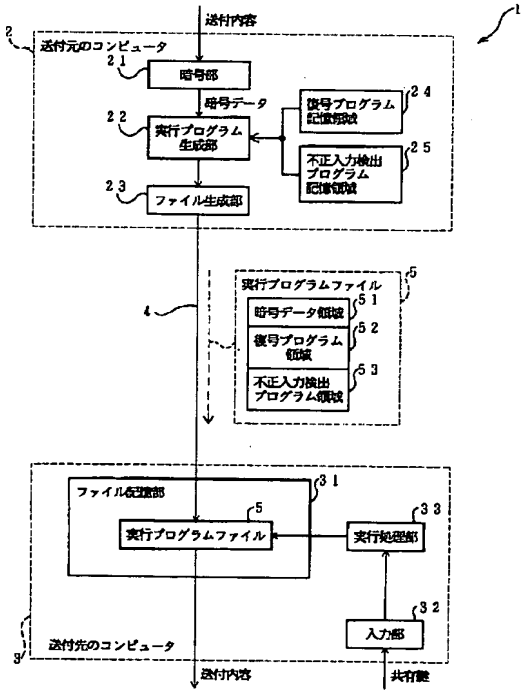
(74)代理人　弁理士　原　謙三

(54)【発明の名称】　暗号データの送付用ファイル生成装置、そのプログラムが記録された記録媒体、および、暗号データの送付用ファイルが格納された記録媒体

(57)【要約】

【課題】　送付先に限定されず、かつ、安全に送付可能な暗号データ送付システムを提供する。

【解決手段】　送付元のコンピュータ２において、実行プログラム生成部２２は、送付内容を示す暗号データと復号プログラムとを含む実行プログラムを生成する。当該実行プログラムは、送付先のコンピュータ３で実行可能な実行プログラムファイル５として、コンピュータ３へ送付される。コンピュータ３にて、実行プログラムファイル５の実行が指示され、正しい共有鍵が入力されると、上記復号プログラムは、暗号データを復号する。実行プログラムファイル５は、他の用途の実行プログラムと同じ形式なので、暗号データ自体を送付する場合よりも安全に送付できる。また、実行プログラムファイル５に復号プログラムも格納されているので、コンピュータ３に予め復号プログラムを用意せずに、送付内容を伝達できる。



【特許請求の範囲】
【請求項１】送付先で実行可能な実行プログラムが格納された送付用ファイルを生成するファイル生成部を備え、
上記実行プログラムは、暗号化されたデータと、正しい復号鍵が入力された場合に当該暗号データを復号する復号プログラムとを含んでいることを特徴とする暗号データの送付用ファイル生成装置。
【請求項２】上記実行プログラムには、さらに、認証プログラムが含まれており、
当該認証プログラムは、実行したときの入力に基づいて、当該実行プログラムの実行者を認証し、認証に失敗した場合、上記復号プログラムの実行を阻止することを特徴とする請求項１記載の暗号データの送付用ファイル生成装置。
【請求項３】上記実行プログラムには、さらに、不正入力検出プログラムが含まれており、
当該不正入力検出プログラムは、所定の回数、不正な入力を検出した場合、当該実行プログラムが格納されたファイルを書き換えて、上記復号プログラムの実行を阻止することを特徴とする請求項１または２記載の暗号データの送付用ファイル生成装置。
【請求項４】さらに、予め定められた複数の暗号アルゴリズムの中から、暗号化に使用する暗号アルゴリズムを選択する選択部と、
選択された暗号アルゴリズムにて、送付内容を暗号化する暗号部とを備え、
上記ファイル生成部は、選択された暗号アルゴリズムに応じた復号プログラムを選択して、上記送付用ファイルを生成することを特徴とする請求項１、２または３記載の暗号データの送付用ファイル生成装置。
【請求項５】暗号化されたデータの送付用ファイルを生成するファイル生成部を実現するためのプログラムが記録されており、
上記送付用ファイルは、送付先で実行可能な実行プログラムを格納し、
上記実行プログラムには、上記暗号データと、正しい復号鍵が入力された場合に当該暗号データを復号する復号プログラムとが含まれていることを特徴とするプログラムが記録された記録媒体。
【請求項６】暗号化された暗号データの送付用ファイルが格納された記録媒体であって、
上記送付用ファイルには、実行プログラムが格納されており、
上記実行プログラムは、上記暗号データと、正しい復号鍵が入力された場合に当該暗号データを復号する復号プログラムとを含み、読み出し先で実行が指示された場合、入力される復号鍵に基づいて、上記復号プログラムに上記暗号データを復号させることを特徴とする暗号データの送付用ファイルが格納された記録媒体。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信路や記録媒体などを介した暗号データの送付に好適な送付用ファイルを作成できる暗号データの送付用ファイル生成装置、そのプログラムが記録された記録媒体、および、当該送付用ファイルが格納された記録媒体に関するものである。
【０００２】
【従来の技術】近年におけるインターネットの普及に伴って、各コンピュータ間のデータ送受は、より一層容易になりつつある。一方、特に対策を講じない限り、第三者によるデータの不正アクセスも容易になるので、例えば、データの漏洩、破壊、あるいは改竄などの被害も増加する傾向にある。したがって、重要なデータを保護するために、暗号技術が従来より利用されている。
【０００３】具体的には、例えば、秘密鍵（共有鍵）暗号方式の場合、暗号データの送付に先立って、送付先のコンピュータと送付元のコンピュータとの間で、暗号鍵が共有される。また、両コンピュータ間で、暗号および復号に使用する暗号アルゴリズムの種類が決められ、送付元のコンピュータには、当該暗号アルゴリズムに対応する暗号プログラムが用意されると共に、送付先のコンピュータには、当該暗号アルゴリズムに対応する復号プログラムが用意される。
【０００４】その後、送付元のコンピュータは、当該共有鍵で送付内容を暗号化して送付する。一方、送付先のコンピュータでは、上記共有鍵をパラメータとして、上記復号プログラムが実行され、受け取った暗号データは、送付内容を示すデータへと復号される。ここで、共有鍵を知らない第三者は、送付される暗号データを正しく復号できないので、送付内容を安全に伝えることができる。
【０００５】
【発明が解決しようとする課題】しかしながら、上記従来の暗号データの送付方法では、送付先のコンピュータが送付元と同じ暗号アルゴリズムの復号プログラムまたは装置を持っていないと、暗号データを正しく送付できないという問題を有している。
【０００６】したがって、例えば、異なった復号プログラムを有するコンピュータなど、所定の復号プログラムを持たないコンピュータには、暗号データを送付できず、暗号データの送付範囲が限定されてしまう。
【０００７】また、各コンピュータへ確実に暗号データを送付するためには、例えば、送付元のコンピュータが予め復号プログラムを送付先に配付したり、送付先のコンピュータが予め復号プログラムを所定の場所からダウンロードするなどして、復号プログラムを用意する必要がある。この結果、送付先の数が増加するに伴って、復号プログラムを用意する手間が増大する。
【０００８】さらに、暗号アルゴリズムの種類を変更す

る場合、個々の送付先に、新たな復号プログラムを用意する必要があり、非常に手間がかかる。したがって、暗号アルゴリズムの種類は、固定されがちになり、第三者に漏洩しやすくなる。加えて、上記従来の送付方法では、送付元と送付先との双方が暗号アルゴリズムの種類を把握しているので、暗号アルゴリズムの種類を秘匿することは、さらに困難である。この結果、第三者は、暗号アルゴリズムに適した解読方法を選択しやすく、暗号データの秘匿性が低下する。

【０００９】加えて、送付先において、使用者は、暗号データに応じた復号プログラムの実行を指示すると共に、当該暗号データと共有鍵との双方を正しく指定する必要があり、復号時の操作が煩雑になる。なお、暗号データを格納したファイルの拡張子や、暗号データを送受する際のＭＩＭＥ（Multipurpose Internet Mail Extensions）タイプなどを指定すれば、復号プログラムを指定できる。ところが、この場合は、復号プログラムが第三者にも公開されるので、暗号データの秘匿性がさらに低下する。

【００１０】また、特に、インターネットでは、暗号化されたデータが特定のポートで送受されるため、第三者は、インターネット上を伝送されるデータの中から、暗号データを識別しやすい。したがって、暗号データが、盗聴や改竄などの攻撃対象になりやすく、暗号データの秘匿性がさらに低下する。

【００１１】本発明は、上記の問題点に鑑みてなされたものであり、その目的は、送付先に限定されず、かつ、安全に送付可能な送付用ファイルを作成できる暗号データの送付用ファイル生成装置、そのプログラムが記録された記録媒体、および、上記送付ファイルが格納された記録媒体を提供することにある。

【００１２】

【課題を解決するための手段】請求項１の発明に係る暗号データの送付用ファイル生成装置は、上記課題を解決するために、送付先で実行可能な実行プログラムが格納された送付用ファイルを生成するファイル生成部を備え、上記実行プログラムは、暗号化されたデータと、正しい復号鍵が入力された場合に当該暗号データを復号する復号プログラムとを含んでいることを特徴としている。

【００１３】上記構成によれば、ファイル生成部は、暗号化された暗号データと、当該暗号データの復号プログラムとを含む実行プログラムを作成し、例えば、実行プログラムファイルや、当該実行プログラムファイルをさらに圧縮したファイルなど、実行プログラムを示す送付用ファイルを生成する。

【００１４】当該送付用ファイルは、インターネットなどの通信路、または、ディスクなどの記録媒体を介して、送付先に送付される。送付用ファイルが正規の送付先に届けられ、送付用ファイルに格納された実行プログラムの実行が指示されると、当該実行プログラムは、復号プログラムを実行させる。復号プログラムは、正しい復号鍵が入力された場合、上記実行プログラムに含まれる暗号データを復号する。なお、復号鍵の入力は、例えば、実行プログラムの実行を指示する際の引数や、実行中のキー入力、あるいは、特定のファイルからの入力など、種々の方法で入力される。これにより、正規の送付先では、暗号データを正しく復号できる。一方、復号鍵を知らない第三者は、送付用ファイルを入手したとしても、暗号データを正しく復号できない。したがって、正規の送付先のみに、安全に送付内容を伝達できる。

【００１５】上記構成によれば、送付用ファイルに、復号プログラムを含む実行プログラムが格納されている。したがって、暗号データの作成時と同じ暗号アルゴリズムの復号プログラムや復号装置が、送付先に予め用意されていなくても、送付先は、何ら支障なく暗号データを復号できる。この結果、従来よりも広い範囲に暗号化されたデータを送付できる。また、送付先の用意が不要なので、送付範囲を広げる際の手間を削減できる。

【００１６】さらに、復号プログラムや復号装置を送付先に予め用意しなくても、暗号データを送付できるので、暗号アルゴリズムを切り換える際の手間は、従来に比べて大幅に削減される。したがって、送付元は、頻繁に暗号アルゴリズムを変更でき、暗号データを送付する際の安全性をさらに向上できる。

【００１７】また、暗号化されたデータは、通信路や記録媒体などの送付経路上を、実行プログラムが格納されたファイルとして送付されている。ここで、実行プログラムは、不特定多数に公開されている場合もあり、一般に、暗号化されたデータに比べて重要でないものが多い。したがって、実行プログラムが格納されたファイルとして送付した場合、暗号データ自体を送付する場合に比べて、第三者の注意を引きにくく、攻撃対象となりにくい。この結果、暗号データ自体を送付する場合よりも安全性を向上できる。

【００１８】なお、実行プログラムが格納されているので、例えば、正しく復号鍵が入力されなかった場合に復号とは異なるプログラムを実行させることもできる。この場合は、他の用途のプログラムが格納されたファイルとの区別が、さらにつきにくくなるので、より一層安全性を向上できる。

【００１９】加えて、上記実行プログラムの実行が指示された場合、当該実行プログラムの復号プログラムが動作して暗号データを復号する。したがって、送付先では、実行プログラムの実行を指示し、かつ、正しい復号鍵を入力するだけで、暗号データを復号できる。この結果、送付先にて、暗号データに応じた復号プログラムを指定する手間がなくなり、操作を簡略化できる。

【００２０】さらに、復号プログラムが含まれているので、送付元が送付先へ暗号アルゴリズムの種類を伝えな

くても、暗号データを復号できる。したがって、送付先の使用者や送付経路から、暗号アルゴリズムの種類が漏洩する虞れがない。この結果、暗号データを送付する際の安全性をさらに向上できる。

【００２１】請求項２の発明に係る暗号データの送付用ファイル生成装置は、請求項１記載の発明の構成において、上記実行プログラムには、さらに、認証プログラムを含んでおり、当該認証プログラムは、実行したときの入力に基づいて、当該実行プログラムの実行者を認証し、認証に失敗した場合、上記復号プログラムの実行を阻止することを特徴としている。

【００２２】上記構成において、送付用ファイル生成装置で生成された送付用ファイルが送付先に届けられ、当該送付用ファイル内の実行プログラムが実行されると、当該実行プログラムは、上記認証プログラムを実行させる。当該認証プログラムは、実行プログラムの実行者を認証し、認証に失敗した場合、復号プログラムの実行を阻止する。なお、認証時の入力は、復号鍵の入力と同様に、例えば、キー入力や引数、特定のファイルなど、種々の方法で入力される。したがって、暗号データは、特定の実行者が実行プログラムの実行を指示した場合にのみ、正しく復号される。この結果、実行者を特定でき、暗号データを送付する際の安全性をさらに向上できる。

【００２３】請求項３の発明に係る暗号データの送付用ファイル生成装置は、請求項１または２記載の発明の構成において、上記実行プログラムには、さらに、不正入力検出プログラムが含まれており、当該不正入力検出プログラムは、所定の回数、不正な入力を検出した場合、当該実行プログラムが格納されたファイルを書き換えて、上記復号プログラムの実行を阻止することを特徴としている。なお、書き換えられるファイルは、例えば、送付ファイル自体や、送付ファイルから生成した実行プログラムファイルなど、実行プログラムが格納されたファイルである。

【００２４】上記構成において、送付用ファイル生成装置で生成された送付用ファイルが送付先に届けられ、当該送付用ファイル内の実行プログラムが実行されると、当該実行プログラムは、不正入力検出プログラムを実行させる。当該不正入力検出プログラムは、復号鍵の入力や認証用の入力を監視して、所定の回数、不正な入力を検出した場合、当該実行プログラムが格納されたファイルを書き換えて、上記復号プログラムの実行を阻止する。

【００２５】なお、書き換える際、上記ファイル全体を消去してもよいし、ファイルのうち、復号プログラムの実行に不可欠な部分のみを変更してもよい。また、上記回数の数え方は、実行プログラムが実行される毎に、数え直してもよいし、通算して数えてもよい。なお、通算して数える場合は、例えば、上記ファイルの一部など、実行プログラムが終了してもデータを保持可能な領域に、通算回数を示すデータが格納される。

【００２６】上記構成によれば、不正な入力が所定の回数繰り返された場合、実行プログラムを格納したファイルが書き換えられる。したがって、書換え後に正しい入力が行われても、暗号データを復号できない。これにより、試行錯誤で正しい入力を推定することもできなくなり、さらに安全性を向上できる。

【００２７】ところで、上記暗号データは、例えば、予め作成された暗号データファイルとして、送付用ファイル生成装置に与えられてもよいし、送付用ファイル生成装置が、与えられた送付内容を暗号化して生成してもよい。また、ファイル生成部が、暗号アルゴリズムに応じた復号プログラムを添付できれば、任意の暗号アルゴリズムを使用できる。

【００２８】ただし、例えば、暗号データファイルの拡張子や内容、あるいは、使用者の指示などによって、送付用ファイル生成装置へ暗号アルゴリズムの種類を指示する場合、暗号アルゴリズムの種類が送付用ファイル生成装置の使用者から漏洩する虞れがある。また、使用者が暗号アルゴリズムを選択すると、それぞれの使用頻度が不均等になることが多く、暗号アルゴリズムの種類を推測されやすくなる。いずれの場合であっても、暗号アルゴリズムの種類が特定されると、暗号データが解読されやすくなり、安全性が低下する。

【００２９】これに対して、請求項４の発明に係る暗号データの送付用ファイル生成装置は、請求項１、２または３記載の発明の構成において、さらに、予め定められた複数の暗号アルゴリズムの中から、暗号化に使用する暗号アルゴリズムを選択する選択部と、選択された暗号アルゴリズムにて、送付内容を暗号化する暗号部とを備え、上記ファイル生成部は、選択された暗号アルゴリズムに応じた復号プログラムを選択して、上記送付用ファイルを生成することを特徴としている。

【００３０】上記構成に係る送付用ファイル生成装置は、複数の暗号アルゴリズムのうちのいずれかを用いて送付内容を暗号化し、送付用ファイルが生成される。それゆえ、送付用ファイル生成装置の使用者であっても、暗号アルゴリズムの種類を特定できない。さらに、各暗号アルゴリズムの使用頻度は、使用者の嗜好に拘わらず設定される。これらの結果、暗号データの作成に使用された暗号アルゴリズムの種類をさらに確実に秘匿でき、安全性を向上できる。

【００３１】一方、請求項５の発明に係るプログラムが記録された記録媒体は、上記課題を解決するために、暗号化されたデータの送付用ファイルを生成するファイル生成部を実現するためのプログラムが記録されており、上記送付用ファイルは、送付先で実行可能な実行プログラムを格納し、上記実行プログラムには、上記暗号データと、正しい復号鍵が入力された場合に当該暗号データを復号する復号プログラムとが含まれていることを特徴

としている。

【００３２】上記構成の記録媒体に記録されたプログラムがコンピュータにより実行されると、上記ファイル生成部は、送付先で実行可能な実行プログラムが格納された送付用ファイルを生成する。当該実行プログラムには、上記暗号データと復号プログラムとが含まれているので、当該送付用ファイルを送付することによって、請求項１と同様に、送付先に限定されず、かつ、安全に暗号データを送付できる。

【００３３】また、請求項６の発明に係る暗号データの送付用ファイルが格納された記録媒体は、上記課題を解決するために、上記送付用ファイルには、実行プログラムが格納されており、上記実行プログラムは、上記暗号データと、正しい復号鍵が入力された場合に当該暗号データを復号する復号プログラムとを含み、読み出し先で実行が指示された場合、入力される復号鍵に基づいて、上記復号プログラムに上記暗号データを復号させることを特徴としている。

【００３４】上記構成において、コンピュータが上記記録媒体から送付用ファイルを読み取り可能になり、当該送付用ファイル内の実行プログラムの実行が指示されると、実行プログラム中の復号プログラムが実行される。当該復号プログラムは、正しい入力鍵が入力された場合、実行プログラム中の暗号データを正しく復号する。それゆえ、当該記録媒体を介して送付することによって、請求項１と同様に、送付先に限定されず、かつ、安全に暗号データを送付できる。

【００３５】

【発明の実施の形態】〔第１の実施形態〕本発明の一実施形態について図１ないし図４に基づいて説明すると以下の通りである。すなわち、図１に示すように、本実施形態に係る暗号データ送付システム１は、暗号化されたデータの送付元となるコンピュータ２と、当該データを受け取る送付先のコンピュータ３とを備えており、暗号化されたデータは、送付路４を介し、実行プログラムファイル５として送付される。上記送付路４は、例えば、インターネットなどの通信路、あるいは、磁気ディスクなどの持ち運び可能な記録媒体であり、上記実行プログラムファイル５を届けることができる。なお、上記実行プログラムファイル５が特許請求の範囲に記載の送付用ファイルに対応し、コンピュータ２が送付用ファイル生成装置に対応している。

【００３６】上記送付元のコンピュータ２は、所定の暗号アルゴリズムで送付内容を暗号化する暗号部２１と、生成された暗号データに基づいて、上記送付先のコンピュータ３が実行可能な実行プログラムを生成する実行プログラム生成部２２と、当該実行プログラムをファイルとして出力するファイル生成部２３とを備えている。さらに、コンピュータ２には、例えば、半導体メモリやディスク装置などの記憶装置の一領域として、復号プログラム記憶領域２４および不正入力検出プログラム記憶領域２５が設けられている。

【００３７】上記各部２１ないし２３は、コンピュータ２のＣＰＵが所定のプログラムを実行することで実現される機能ブロックであってもよいし、同様の動作を行うハードウェアとして実現することもできる。ただし、ソフトウェアで実現した場合は、上記各プログラムを記録媒体や通信路で配付し、通常のコンピュータで実行することにより、上記各部２１ないし２３を実現できるので、配付が容易になる。なお、実行プログラム生成部２２およびファイル生成部２３が特許請求の範囲に記載のファイル生成部に対応している。

【００３８】上記暗号部２１の暗号アルゴリズムは、例えば、ＤＥＳ（Data Encryption Standard）、ＩＤＥＡ（International Data Encryption Algorithm）あるいはＲＣ５などの秘密鍵暗号方式であり、例えば、送付元から送付先へ秘密に通知するなどして、送付元および送付先は、実行プログラムファイル５を送付するまでの間に共有鍵を共有している。なお、秘密鍵暗号方式では、暗号データを暗号化する際の暗号鍵と、復号する際の復号鍵とが共通なので、以下では、両者を特に区別せず、共有鍵と称する。

【００３９】上記両プログラム記憶領域２４・２５は、上記コンピュータ３で実行可能なプログラムを記憶しており、復号プログラム記憶領域２４には、上記暗号データを復号するための復号プログラムが格納されている。また、不正入力検出プログラム記憶領域２５には、復号時の不正な入力を検出する不正入力検出プログラムが格納されている。なお、各プログラムは、送付先のコンピュータ３で実行できれば、送付元のコンピュータ２で実行できなくてもよい。

【００４０】さらに、上記実行プログラム生成部２２は、例えば、上記各プログラム記憶領域２４・２５から読み出したプログラムに、暗号部２１から受け取った暗号データを付加するなどして実行プログラムを生成する。なお、実行プログラム生成部２２は、読み出したプログラム中に暗号データに応じて変動する部分が存在する場合、暗号部２１から受け取った暗号データに基づいて当該部分を調整して実行プログラムを生成する。また、ファイル生成部２３は、当該実行プログラムを図示しない記録媒体に書き込むなどして、実行プログラムファイル５を生成できる。当該実行プログラムファイル５は、他の用途で使用される実行プログラムファイルと同一形式のバイナリファイルであり、一見しただけでは両者を区別できない。

【００４１】なお、図１では、説明の便宜上、各プログラム記憶領域２４・２５、並びに、後述の各領域５２・５３を明確に区別しているが、多くの場合、不正入力検出プログラムは、復号プログラムの一部であり、各領域２５（５３）は、各領域２４（５２）の一部として実現

されている。また、上記では、各プログラム領域２４・２５にプログラム自体が格納されている場合を例にして説明したが、プログラムを生成するためのデータが格納されていてもよい。同一内容の実行プログラムファイル５を生成できれば、格納方法に拘わらず、同様の効果が得られる。

【００４２】一方、送付先のコンピュータ３には、受け取った実行プログラムファイル５を格納するファイル記憶部３１と、使用者からの入力を受け付ける入力部３２と、入力部３２の指示に応じて、ファイル記憶部３１内の実行プログラムファイル５を実行する実行処理部３３とが設けられている。上記ファイル記憶部３１は、実行処理部３３により読み出し可能であれば、例えば、ハードディスクなど、コンピュータ３に備えつけられた記憶装置でもよいし、持ち運び可能な記録媒体であってもよい。

【００４３】上記入力部３２は、例えば、マウスやキーボードなどの入力装置と、例えば、シェルなどのユーザインターフェースプログラムとなどから構成されており、使用者から、実行プログラムファイル５の実行指示を受け取ることができる。また、上記実行処理部３３は、例えば、オペレーティングシステム（ＯＳ）の一機能として実現されており、入力部３２から実行指示を受け取った場合、例えば、ＯＳで規定された方法で実行プログラムファイル５を内部メモリに展開するなどして、実行プログラムファイル５に格納されたプログラムを実行する。なお、ファイル記憶部３１内の実行プログラムファイル５を実行した場合に、後述する各機能ブロック５２Ｘ・５３Ｘを形成できれば、他の構成の入力部３２および実行処理部３３を使用しても同様の効果が得られる。

【００４４】上記構成の暗号データ送付システム１において、送付元のコンピュータ２から送付先のコンピュータ３へ送付内容が伝達される際の動作について説明すると以下の通りである。すなわち、図２のＳ１に示すように、送付元のコンピュータ２の暗号部２１に送付内容が与えられると、暗号部２１は、予め定められた共有鍵を用いて、送付内容を暗号化する（Ｓ２）。なお、共有鍵は、例えば、コンピュータ２に予め格納されたものを使用してもよいし、コンピュータ２の使用者が、その都度入力してもよい。

【００４５】さらに、実行プログラム生成部２２は、Ｓ３において、暗号部２１から受け取った暗号データと、復号プログラム記憶領域２４および不正入力検出プログラム記憶領域２５から読み出したプログラムとに基づいて、実行プログラムを生成し、ファイル生成部２３は、Ｓ４において、当該実行プログラムを実行プログラムファイル５として出力する。

【００４６】これにより、図１に示すように、コンピュータ２において、上記暗号データが格納された暗号データ領域５１と、復号プログラムが格納された復号プログラム領域５２と、不正入力検出プログラムが格納された不正入力検出プログラム領域５３とを有する実行プログラムファイル５が生成される。当該実行プログラムファイル５は、Ｓ５において、記録媒体の輸送や通信など、種々の方法を用いて、送付先のコンピュータ３へ送付される。

【００４７】一方、送付先のコンピュータ３では、受け取った実行プログラムファイル５がファイル記憶部３１に格納される（Ｓ６）。さらに、使用者の指示などにより、実行プログラムファイル５の実行が指示されると（Ｓ７）、実行処理部３３は、実行プログラムファイル５内の実行プログラムを実行させる（Ｓ８）。これにより、暗号データ領域５１内の暗号データは、復号プログラム領域５２内の復号プログラムにより復号され、コンピュータ３は、送付内容を取得できる。

【００４８】具体的には、上記Ｓ８において、実行処理部３３は、実行プログラムファイル５に基づき、図３に示す機能ブロックをコンピュータ３に追加する。これにより、図４のＳ１１ないしＳ１６の処理が行われる。なお、復号部５２Ｘおよび不正入力検出部５３Ｘは、コンピュータ３が、復号プログラム領域５２の復号プログラムおよび不正入力検出プログラム領域５３の不正入力検出プログラムを実行することによって実現される機能ブロックである。また、図４に示すステップＳ１１ないしＳ１４が、特許請求の範囲に記載の復号プログラムに対応しており、Ｓ１３、Ｓ１５およびＳ１６が不正入力検出プログラムに対応している。

【００４９】すなわち、実行が指示されると、上記復号部５２Ｘは、例えば、表示などによって、共有鍵の入力を要求する（Ｓ１１）。Ｓ１２において、使用者が入力部３２により共有鍵を入力すると、Ｓ１３において、不正入力検出部５３Ｘは、当該共有鍵が正しいか否かを判定する。

【００５０】正しい共有鍵が入力された場合は、復号部５２Ｘは、当該共有鍵を用いて、上記暗号データ領域５１の暗号データを正しい送付内容に復号する（Ｓ１４）。一方、不正な共有鍵が入力された場合、不正入力検出部５３Ｘは、不正な入力の回数が所定の値を越えているか否かを判定する（Ｓ１５）。ここで、入力回数として、実行プログラムファイル５がファイル記憶部３１に格納されてからの通算回数を数える場合、不正入力検出部５３Ｘは、例えば、実行プログラムファイル５の一部領域など、実行プログラムの実行が終了しても記憶内容が保存される領域へ通算回数を保存しておき、当該領域の値を参照して判定する。

【００５１】上記Ｓ１５において、入力回数が所定の値を越えていた場合、不正入力検出部５３Ｘは、それ以降に実行プログラムファイル５の実行が指示されても復号部５２Ｘが正常に動作しないように、実行プログラムフ

ファイル５の内容を変更して終了する（Ｓ１６）。なお、変更方法は、実行プログラムファイル５自体をファイル記憶部３１から消去してもよいし、実行プログラムファイル５のうち、正しい復号部５２Ｘを形成するために不可欠なデータが格納されている領域を書き換えてもよい。一方、上記Ｓ１５にて、所定の回数を越えていない場合は、Ｓ１６の処理を行うことなく終了する。

【００５２】上記構成によれば、送付路４で送付される実行プログラムファイル５は、暗号化されているので、共有鍵を知らない第三者は、送付内容を傍聴したり、破壊あるいは改竄することが難しい。さらに、上記実行プログラムファイル５は、内容の重要度が暗号データよりも低いことが多い実行プログラムファイルなので、第三者の注意を引きにくく、攻撃対象となる虞れが低い。これらの結果、送付元のコンピュータ２は、送付内容を安全に送付できる。

【００５３】なお、上記実行プログラムファイル５は、他の用途の実行プログラムファイルと同一の形式であり、暗号データ伝送用のポートを使用せずに伝送される。この結果、送付路４として、暗号データの識別が容易なインターネットを使用する場合であっても、送付内容を目立たずに送付できる。

【００５４】また、上記実行プログラムファイル５には、実行プログラムが格納されているので、復号プログラム以外のプログラムを含ませることができる。一例として、後述する認証プログラムのように、暗号データを送付する際の安全性を直接向上させるためのプログラムを追加すれば、復号時の安全性を向上できる。

【００５５】さらに、認証プログラムに代えて、または、認証プログラムに加えて、ダミープログラムを追加することもできる。当該ダミープログラムは、例えば、画像表示プログラムや音声出力プログラムなど、ファイルサイズが比較的大きくても不審を招かないプログラムが好ましく、実行プログラムファイルの実行時に共有鍵などが正しく指定されなかった場合に実行される。この場合は、実行プログラムファイル５は、一見、他の用途のプログラムファイルと同様の動作を行うので、第三者が暗号データが含まれていないと誤認しやすい。この結果、当該実行プログラムファイル５は、第三者の攻撃対象から外れやすくなり、暗号データを送付する際の安全性をさらに向上できる。なお、この場合、他の用途のプログラムと混同しやすいように、復号プログラムおよび認証プログラムは、例えば、実行を指示する際の引数を入力にするなどして、使用者に入力を要求しない方がよい。

【００５６】また、送付元のコンピュータ２が送付する実行プログラムファイル５には、暗号データと当該暗号データを復号するための復号プログラムとを含む実行プログラムが格納されている。したがって、送付先のコンピュータ３は、暗号データに応じた復号プログラムや装置が予め用意されていない場合であっても、送付された実行プログラムファイル５を実行するだけで暗号データを復号できる。この結果、従来とは異なり、暗号化する際の暗号アルゴリズムの種類によって、暗号データの送付範囲が限定されず、送付範囲を広げる際の手間を削減できる。

【００５７】さらに、暗号アルゴリズムの種類を変更しても、送付先のコンピュータ３に新たな復号プログラムや装置を用意する必要がないので、暗号アルゴリズムの種類を頻繁に変更できる。さらに、送付先では、暗号化に使用した暗号アルゴリズムの種類に拘わらず、実行プログラムファイル５の実行を指示するだけである。したがって、送付先の使用者あるいはコンピュータ３は、上記暗号アルゴリズムの種類を把握する必要が無い。これらの結果、暗号アルゴリズムの種類を秘匿しやすくなり、送付時の安全性をさらに向上できる。

【００５８】加えて、送付先のコンピュータ３では、上記実行プログラムファイル５の実行を指示し、正しい共有鍵を入力するだけで、暗号データを復号できる。したがって、送付された暗号データと、当該暗号データに対応した復号プログラムと、復号鍵とを指示する必要のある従来技術に比べて、コンピュータ３の操作を簡略化できる。また、暗号データと復号プログラムとが同一の実行プログラムファイル５に格納されているので、それぞれを別のファイルで送付する場合よりも、両コンピュータ２・３および送付路４におけるファイル管理が容易になる。

【００５９】なお、上記の説明では、Ｓ１１およびＳ１２に示すように、実行プログラムファイル５の実行中に、使用者が共有鍵を入力する場合を例にして説明したが、これに限るものではない。上記Ｓ１１およびＳ１２に代えて、例えば、予め用意されたファイルから共有鍵を読み込めば、共有鍵を入力する際の手間を削減できる。また、実行プログラムファイル５の実行を指示する際、例えば、実行プログラムファイル５のファイル名に加えて、共有鍵を引数として入力してもよい。いずれの場合であっても、復号部５２Ｘが暗号データを復号するまでの間に、共有鍵が入力されれば、本実施形態と同様の効果が得られる。

【００６０】また、上記Ｓ７では、使用者によって、実行プログラムファイル５の実行が指示される場合を例にして説明したが、例えば、ファイル記憶部３１へ実行プログラムファイル５が格納されたことを検出するなどして、実行処理部３３が能動的に実行プログラムを実行させてもよい。

【００６１】ところで、本実施形態の実行プログラムファイル５には、復号プログラムに加えて、不正入力検出部５３Ｘを形成するためのプログラムも含まれている。それゆえ、不正な入力を検出した場合、それ以降は正常に実行できないように、実行プログラムファイル５を変

更できる。この結果、第三者が共有鍵の入力を繰り返しても、送付内容を復号できず、さらに安全性を向上できる。

【００６２】ここで、上記Ｓ１６を実行するまでの回数が小さ過ぎると、正規の使用者が入力ミスした場合に、復号プログラムを実行できなくなる。一方、大き過ぎる場合は、第三者が、偶然、正しい共有鍵を入力して、送付内容が漏洩する可能性がある。したがって、上記回数は、例えば、数回程度など、両者のバランスを取った値に設定される。

【００６３】なお、上記Ｓ１５およびＳ１６の処理の後で終了せずに上記Ｓ１１の処理を行い、再度、共有鍵の入力を要求することもできる。この場合は、上記Ｓ１５にて、実行プログラムファイル５を実行する毎に、入力回数を数え直してもよい。当然ながら、数え直す場合には、通算回数を保存する必要がない。

【００６４】〔第２の実施形態〕本実施形態では、実行プログラムが、さらに認証プログラムを含んでいる場合について説明する。

【００６５】すなわち、図５に示すように、本実施形態に係る暗号データ送付システム１ａでは、送付元のコンピュータ２ａに認証プログラム記憶領域２６ａが追加されており、実行プログラム生成部２２ａは、当該認証プログラム記憶領域２６ａの内容をも参照して、実行プログラムファイル５ａを生成できる。これにより、図１に示す各領域５１ないし５３に加えて、認証プログラム領域５４ａを有する実行プログラムファイル５ａが生成される。なお、送付元のコンピュータ２ａの残余の構成、並びに、送付先のコンピュータ３の構成は、図１に示す構成と同一なので、同じ機能を有する部材には、同じ参照符号を付して説明を省略する。

【００６６】上記構成の暗号データ送付システム１ａでは、図１に示す暗号データ送付システム１と同様に、図２に示す各ステップが行われ、送付先のコンピュータ３にて実行プログラムファイル５ａが実行される。

【００６７】ただし、実行プログラムファイル５ａには、認証プログラム領域５４ａが追加されているので、実行プログラムファイル５ａの実行が指示された場合、上述のＳ８にて、図６に示す機能ブロックが送付先のコンピュータ３に形成される。具体的には、図３に示す機能ブロックに加えて、復号部５２Ｘと不正入力検出部５３Ｘとの間に、認証部５４Ｘが形成される。なお、当該認証部５４Ｘは、送付先のコンピュータ３が上記認証プログラム領域５４ａに格納されたプログラムを実行することによって実現される機能ブロックである。

【００６８】これにより、図７に示すように、図４に示すステップＳ１１ないしＳ１６よりも前に、Ｓ２１ないしＳ２３の処理が行われ、実行プログラムファイル５ａの実行者が認証される。なお、これらのステップＳ２１ないしＳ２３が特許請求の範囲に記載の認証プログラムに対応している。また、本実施形態では、上述のＳ１３、Ｓ１５およびＳ１６に加えて、Ｓ２３が不正入力検出プログラムに対応している。

【００６９】具体的には、実行が指示されると、認証部５４Ｘは、実行者にパスワードの入力を要求する（Ｓ２１）。Ｓ２２において、実行者が共有鍵の入力と同様の方法でパスワードを入力すると、Ｓ２３において、認証部５４Ｘは、当該パスワードが正しいか否かによって、実行者を認証する。

【００７０】上記認証部５４Ｘが認証する際のアルゴリズムは、例えば、固定パスワードを使用するアルゴリズム、あるいは、チャレンジ＆レスポンス方式や同期方式のワンタイムパスワードを使用するアルゴリズムなど、種々のアルゴリズムを利用できる。ただし、認証部５４Ｘを形成するための認証プログラムは、送付元のコンピュータ２ａにて、予め決定されている。

【００７１】認証に成功すると、上述したＳ１１ないしＳ１６が行われ、復号部５２Ｘは、正しい共有鍵が入力された場合に暗号データを復号する。一方、認証に失敗した場合、上述したＳ１５以降の処理が行われる。これにより、認証に所定の回数だけ失敗すると、実行プログラムファイル５ａが書き換えられ、それ以降は、認証結果および共有鍵に拘わらず、暗号データを復号できなくなる。なお、本実施形態では、上記Ｓ１５にて、認証に失敗した回数と、共有鍵の入力に失敗した回数との合計を数えているが、当然ながら、別々に数えてもよい。

【００７２】上記構成によれば、復号部５２Ｘが暗号データを復号する前に、認証部５４Ｘが実行者を認証する。この結果、実行プログラムファイル５ａの実行者を特定でき、暗号データを送付する際の安全性をさらに向上できる。

【００７３】上記パスワードは、共有鍵とは異なり、認証毎に変更できる。また、認証アルゴリズムを複雑にしても、暗号データの復号速度には影響を与えない。この結果、例えば、共有鍵を長くするなど、暗号アルゴリズムのみで安全性を向上する場合に比べて、効率的に安全性を向上できる。

【００７４】〔第３の実施形態〕ところで、上記第１および第２の実施形態では、暗号化する際の暗号アルゴリズムが１種類の場合を例にして説明したが、これに限るものではない。本実施形態では、複数の暗号アルゴリズムで暗号化でき、さらに、送付元のコンピュータ自体が暗号アルゴリズムを選択する場合について説明する。

【００７５】すなわち、図８に示すように、本実施形態では、送付元のコンピュータ２ｂにおいて、図１に示す構成に加えて、複数の暗号アルゴリズムを選択する選択部２７ｂが設けられている。また、これに伴い、暗号部２１に代えて、複数の暗号アルゴリズムのうち、指示された暗号アルゴリズムにて、送付内容を暗号化できる暗号部２１ｂが設けられており、復号プログラム記憶領域

２４ｂには、各暗号アルゴリズムに対応した復号プログラムが、それぞれ格納されている。なお、残余の部材は、図１に示す構成と同様であるため、同じ機能を有する部材には同じ参照符号を付して説明を省略する。

【００７６】また、本実施形態に係る暗号データ送付システム１ｂにおいて、共有鍵の長さは、各暗号アルゴリズムで使用する共有鍵の最大長以上に設定されており、暗号部２１ｂおよび復号部５２Ｘは、例えば、ビット選択など、所定の演算を用いて、各暗号アルゴリズム用の共有鍵を生成する。これにより、送付元のコンピュータ２ｂおよび送付先のコンピュータ３の使用者は、暗号アルゴリズムに拘わらず、同一の共有鍵によって、暗号／復号を指示できる。なお、共有鍵の長さが長くなると、入力が煩雑になるので、通常は、最大長に設定される。

【００７７】上記構成において、暗号データ送付システム１ｂは、図２に示す各ステップと同様の動作を行う。ただし、図９に示すように、Ｓ１において、送付内容が入力されると、新たに設けられたステップＳ３１において、選択部２７ｂは、予め定められた複数の暗号アルゴリズムの中から、今回使用する暗号アルゴリズムを選択する。一方、Ｓ２において、暗号部２１ｂは、選択された暗号アルゴリズムで送付内容を暗号化する。また、Ｓ３にて、実行プログラム生成部２２が実行プログラムを生成する際、例えば、選択部２７ｂの指示に基づくなどして、当該暗号アルゴリズムに応じた復号プログラムが復号プログラム記憶領域２４ｂから読みだされる。これにより、送付元のコンピュータ２ｂは、使用者の意図に拘わらず、実行プログラムファイル５の作成時の暗号アルゴリズムを毎回変更できる。

【００７８】上記構成によれば、送付元のコンピュータ２ｂが暗号アルゴリズムを選択するので、送付元のコンピュータ２の使用者であっても、暗号アルゴリズムの種類を特定できない。また、使用者が選択する場合とは異なり、各暗号アルゴリズムの使用頻度は、使用者の嗜好に影響されない。これらの結果、暗号アルゴリズムの種類をさらに確実に秘匿できるので、暗号データを送付する際の安全性をさらに向上できる。

【００７９】〔第４の実施形態〕ところで、上記第１ないし第３の実施形態では、実行プログラムファイル自体を送付する場合について説明したが、これに限るものではない。送付されるファイルに実行プログラムが格納されていれば、上記各実施形態と同様の効果が得られる。以下では、実行プログラムファイルを圧縮した圧縮ファイルが送付される場合を例にして、他の形式のファイルを送付する場合を説明する。

【００８０】すなわち、図１０に示すように、本実施形態に係る暗号データ送付システム１ｃでは、送付元のコンピュータ２ｃにおいて、図１に示すファイル生成部２３の代わりに、圧縮ファイル生成部２３ｃが設けられている。当該圧縮ファイル生成部２３ｃは、実行プログラム生成部２２が実行プログラムを生成した場合、例えば、当該実行プログラムを実行プログラムファイル５に格納すると共に、当該実行プログラムファイル５をさらに圧縮するなどして、圧縮ファイル６ｃを生成する。なお、本実施形態では、圧縮ファイル６ｃが特許請求の範囲に記載の送付用ファイルに対応している。

【００８１】圧縮ファイル６ｃは、圧縮時に使用したアルゴリズムを識別するために、通常、ファイル名の拡張子やＭＩＭＥタイプなどが指定されている。ところが、当該圧縮ファイル６ｃに格納された実行プログラムファイル５は、第１の実施形態と同様に、他の実行プログラムファイルと区別がつかない。したがって、第三者には、上記圧縮ファイル６ｃと、他の実行プログラムファイルを圧縮した圧縮ファイルとを識別しにくくなり、実行プログラムファイル５自体を送付する場合と同様の効果が得られる。

【００８２】一方、送付先のコンピュータ３には、実行処理部３３に代えて、圧縮ファイル６ｃ内の実行プログラムファイル５へ実行を指示できる実行処理部３３ｃが設けられている。圧縮ファイル６ｃがファイル記憶部３１へ格納され、実行プログラムファイル５の実行指示が入力部３２を介して伝えられると、実行処理部３３ｃは、例えば、圧縮ファイル６ｃを解凍して、さらに、内部メモリに展開するなどして、図３に示す各機能ブロックを形成する。これにより、第１の実施形態と同様に、正規の使用者は、送付内容を取得できる。

【００８３】なお、上記では、実行処理部３３ｃが、圧縮ファイル６ｃ中の実行プログラムファイル５へ直接実行を指示する場合について説明したが、これに限るものではない。例えば、送付先のコンピュータ３へ、圧縮ファイル６ｃを解凍する解凍部が設けられてもよい。当該解凍部は、使用者の指示に応じて、あるいは、圧縮ファイル６ｃの受領に連動して、圧縮ファイル６ｃを解凍し、実行プログラムファイル５を生成する。実行プログラムファイル５は、ファイル記憶部３１に格納される。この場合は、図１に示す実行処理部３３にて、実行プログラムファイル５の実行を指示できる。なお、この場合、不正入力検出部５３Ｘは、送付される圧縮ファイル６ｃ自体を書き換える代わりに、実行プログラムファイル５を書き換えてもよい。実行プログラムが格納されたファイルを書き換えれば、同様の効果が得られる。

【００８４】また、実行プログラムファイル５を圧縮ファイル６ｃに変換する場合を例にして説明したが、これに限るものではない。送付元のコンピュータは、通信路や記録媒体の特性に応じた種々の形式のファイルを生成してもよい。送付するファイルに、暗号データと復号プログラムとを含む実行プログラムが格納されていれば、同様の効果が得られる。

【００８５】なお、上記第１ないし第４の実施形態では、実行プログラムファイル（５・５ａ）が各領域（５

１・５２・５３・５４ａ）に大別されている場合を例示しているが、各領域の配置は、これに限るものではない。各領域を複数の部分に寸断して混ぜ合わせて配置してもよい。実行が指示された場合、復号プログラムが暗号データを復号可能で、認証プログラムが実行者を認証できるような配置であれば、各領域の配置に拘わらず、同様の効果が得られる。ただし、復号プログラムや認証プログラムの実行速度の点では、暗号データ領域（５１）は、１つの方が望ましい。

【００８６】また、上記各実施形態では、暗号アルゴリズムとして、秘密鍵暗号方式を採用した場合を例にして説明したが、例えば、ＲＳＡ（Rivest Shamir Adleman）暗号方式などの公開鍵暗号方式を使用してもよい。ただし、自らの復号鍵を秘匿するためには、送付先は、暗号アルゴリズムに応じて予め用意されたプログラムまたは装置を用いて、復号鍵から公開の暗号鍵を作成し、送付元に通知する必要がある。一方、送付元が、送付先の復号鍵を予め通知しておけば、上記プログラムや装置を送付先に用意しなくてもよいが、送付先は、自らの復号鍵を秘匿できなくなる。したがって、復号プログラムの速度や規模の点から、秘密鍵暗号方式を採用する方が望ましい。

【００８７】さらに、上記第１、第２および第４の各実施形態では、送付元のコンピュータ（２・２ａ・２ｃ）が送付内容を暗号化する場合を例にして説明したが、これに限るものではない。実行プログラム生成部（２２・２２ａ）へ暗号データが与えられれば、暗号部（２１）がなくても同様の効果が得られる。この場合、実行プログラム生成部は、例えば、暗号データの内容自体、暗号データを示すファイルの拡張子、あるいは、使用者の指示などによって、暗号データの作成時に使用された暗号アルゴリズムを識別して、適切な復号プログラムを添付する。

【００８８】なお、上記第１ないし第４の実施形態では、ファイル記憶部（３１）が送付先のコンピュータ（３）に設けられている場合について説明したが、送付路４が通信路の場合は、ファイル記憶部の一部または全部が、送付元のコンピュータ（２・２ａ・２ｂ・２ｃ）に設けられていてもよい。送付先のコンピュータの入力部（３２）が実行プログラムファイル（５・５ａ）の実行を指示可能で、実行処理部（３３・３３ｃ）がコンピュータ３に各機能ブロック（５２Ｘ・５３Ｘ・５４Ｘ）を追加できれば、上記各実施形態と同様の効果が得られる。

【００８９】さらに、上記各実施形態では、実行プログラムファイルがバイナリファイルの場合を例にしたが、例えば、復号プログラムなどのプログラムの処理内容および暗号データをテキスト形式で表現したファイルであってもよい。実行プログラムファイルの形式に拘わらず、送付先のコンピュータで実行された場合に上記各機能ブロックを形成できれば、同様の効果が得られる。なお、各機能ブロックは、常に形成される必要はなく、必要に応じて形成できればよい。例えば、不正入力検出部（５３Ｘ）が不正な入力を検出した場合は、復号部（５２Ｘ）を形成しなくてもよい。

【００９０】

【発明の効果】請求項１の発明に係る暗号データの送付用ファイル生成装置は、以上のように、実行プログラムが格納された送付用ファイルを生成するファイル生成部を備え、上記実行プログラムは、暗号化されたデータと、正しい復号鍵が入力された場合に当該暗号データを復号する復号プログラムとを含んでいる構成である。

【００９１】上記構成によれば、送付用ファイルに、復号プログラムを含む実行プログラムが格納されているので、送付先は、予め復号プログラムや復号装置を用意せずに、暗号データを送付できる。この結果、送付元となる送付用ファイル生成装置は、送付先に限定されずに、暗号データを送付できるという効果を奏する。

【００９２】さらに、暗号化されたデータは、通信路や記録媒体などの送付経路上を、実行プログラムが格納されたファイルとして送付されているので、第三者の攻撃対象になりにくい。また、送付先では、暗号アルゴリズムの種類に拘わらず、送付用ファイルに格納された実行プログラムの実行を指示するだけなので、暗号アルゴリズムの種類を秘匿できる。これらの結果、暗号データ自体を送付する場合に比べて、安全性を向上できるという効果を併せて奏する。

【００９３】請求項２の発明に係る暗号データの送付用ファイル生成装置は、以上のように、請求項１記載の発明の構成において、上記実行プログラムが認証プログラムを含んでいる構成である。

【００９４】それゆえ、暗号データは、特定の実行者が実行プログラムの実行を指示した場合にのみ、正しく復号される。この結果、実行者を特定でき、暗号データを送付する際の安全性をさらに向上できるという効果を奏する。

【００９５】請求項３の発明に係る暗号データの送付用ファイル生成装置は、以上のように、請求項１または２記載の発明の構成において、上記実行プログラムには、所定の回数、不正な入力を検出した場合、当該実行プログラムが格納されたファイルを書き換えて、上記復号プログラムの実行を阻止する不正入力検出プログラムが含まれている構成である。

【００９６】上記構成によれば、不正な入力が所定の回数繰り返された場合、実行プログラムを格納したファイルが書き換えられる。したがって、書換え後に、正しい入力が行われても、暗号データを復号できない。この結果、第三者が試行錯誤で正しい入力を推定することもできなくなり、さらに安全性を向上できるという効果を奏する。

【００９７】請求項４の発明に係る暗号データの送付用ファイル生成装置は、以上のように、請求項１、２または３記載の発明の構成において、さらに、予め定められた複数の暗号アルゴリズムの中から、暗号化に使用する暗号アルゴリズムを選択する選択部と、選択された暗号アルゴリズムにて、送付内容を暗号化する暗号部とを備えている構成である。

【００９８】それゆえ、送付用ファイル生成装置の使用者が暗号アルゴリズムを指定する場合に比べて、暗号データの作成に使用された暗号アルゴリズムの種類を秘匿でき、安全性をさらに向上できるという効果を奏する。

【００９９】請求項５の発明に係るプログラムが記録された記録媒体は、以上のように、暗号化されたデータの送付用ファイルを生成するファイル生成部を実現するためのプログラムが記録されており、上記送付用ファイルには、暗号データと復号プログラムとを含んだ実行プログラムが格納されている構成である。

【０１００】それゆえ、上記構成の記録媒体に記録されたプログラムを実行し、生成された送付用ファイルを送付することによって、請求項１と同様に、送付先に限定されず、かつ、安全に暗号データを送付できるという効果を奏する。

【０１０１】請求項６の発明に係る暗号データの送付用ファイルが格納された記録媒体は、以上のように、上記送付用ファイルには、実行プログラムが格納されており、上記実行プログラムは、上記暗号データと、正しい復号鍵が入力された場合に当該暗号データを復号する復号プログラムとを含んでいる構成である。

【０１０２】それゆえ、当該記録媒体を介して送付することにより、請求項１と同様に、送付先に限定されず、かつ、安全に暗号データを送付できるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の一実施形態を示すものであり、暗号データ送付システムの要部構成を示すブロック図である。

【図２】上記暗号データ送付システムの動作を示すフローチャートである。

【図３】上記暗号データ送付システムの送付先において、実行プログラムファイルの実行時に形成される機能ブロックを示すブロック図である。

【図４】上記機能ブロックの動作を示すフローチャートである。

【図５】本発明の他の実施形態を示すものであり、暗号データ送付システムの要部構成を示すブロック図である。

【図６】上記暗号データ送付システムの送付先において、実行プログラムファイルの実行時に形成される機能ブロックを示すブロック図である。

【図７】上記機能ブロックの動作を示すフローチャートである。

【図８】本発明のさらに他の実施形態を示すものであり、暗号データ送付システムの要部構成を示すブロック図である。

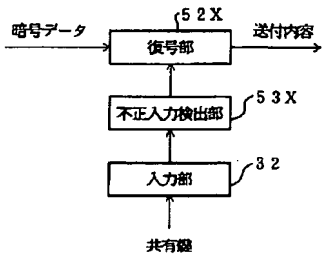
【図９】上記暗号データ送付システムの動作を示すフローチャートである。

【図１０】本発明のまた別の実施形態を示すものであり、暗号データ送付システムの要部構成を示すブロック図である。

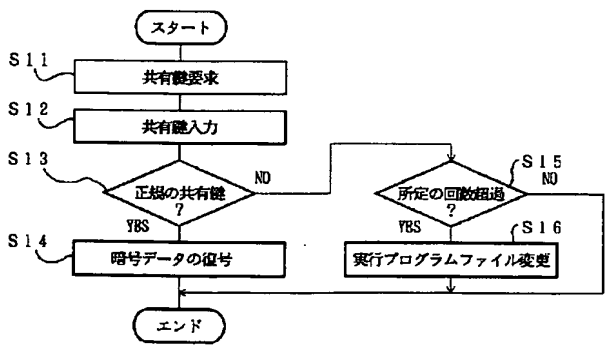
【符号の説明】

２・２ａ・２ｂ・２ｃ　送付元のコンピュータ（送付用ファイル生成装置）
３　送付先のコンピュータ（送付先）
４　送付路（記録媒体）
５・５ａ　実行プログラムファイル（送付用ファイル）
６ｃ　圧縮ファイル（送付用ファイル）
２１ｂ　暗号部
２２・２２ａ　実行プログラム生成部（ファイル生成部）
２３　ファイル生成部
２３ｃ　圧縮ファイル生成部（ファイル生成部）
３１　ファイル記憶部（記録媒体）

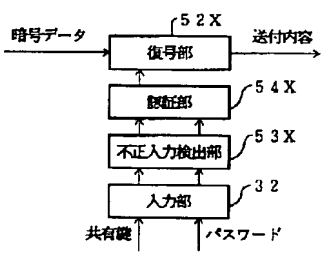
【図３】



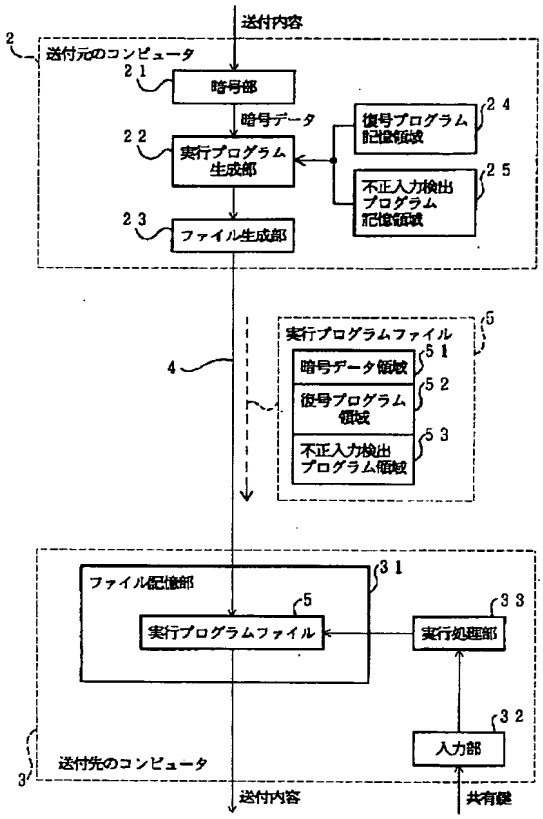
【図４】



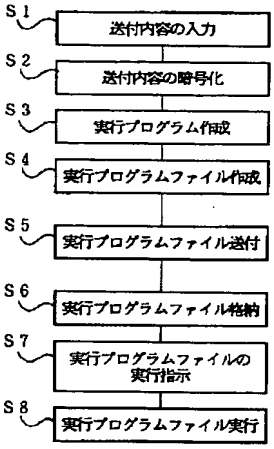
【図６】



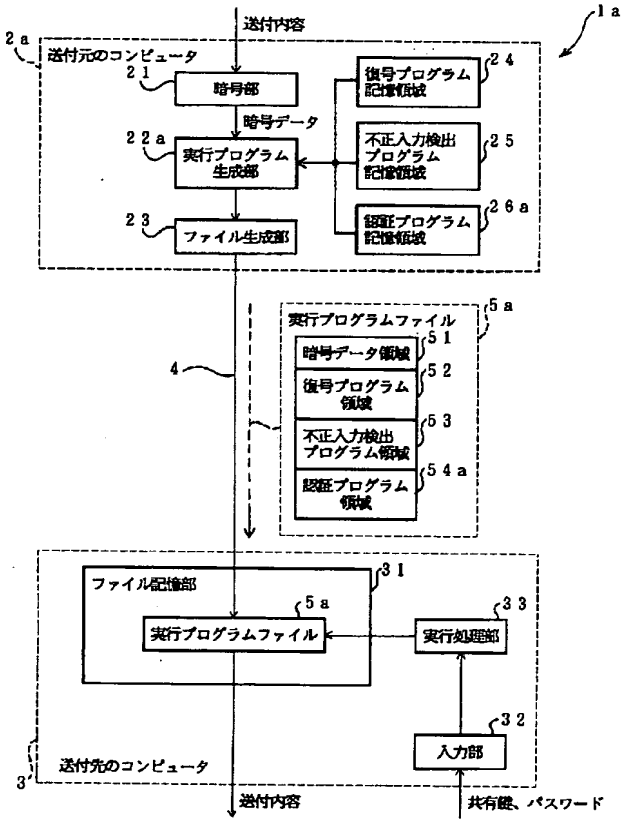
【図１】


送付内容
2
送付元のコンピュータ
21
暗号部
暗号データ
22
実行プログラム生成部
24
復号プログラム記憶領域
25
不正入力検出プログラム記憶領域
23
ファイル生成部
4
5
実行プログラムファイル
51
暗号データ領域
52
復号プログラム領域
53
不正入力検出プログラム領域
31
ファイル記憶部
5
実行プログラムファイル
33
実行処理部
32
入力部
3
送付先のコンピュータ
送付内容
共有鍵

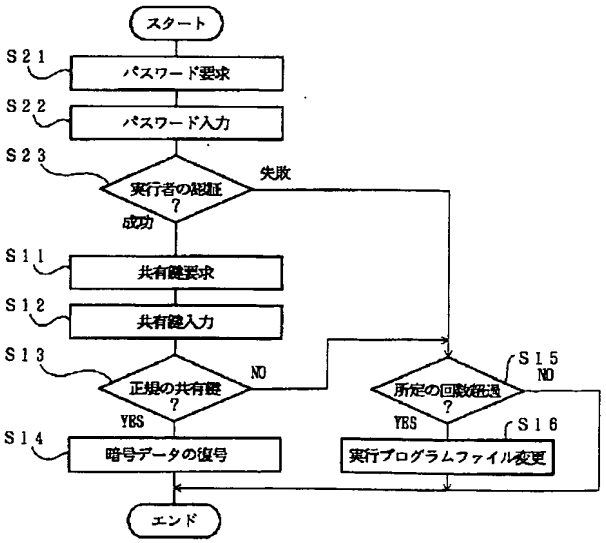
【図２】


1
S1
送付内容の入力
S2
送付内容の暗号化
S3
実行プログラム作成
S4
実行プログラムファイル作成
S5
実行プログラムファイル送付
S6
実行プログラムファイル格納
S7
実行プログラムファイルの実行指示
S8
実行プログラムファイル実行

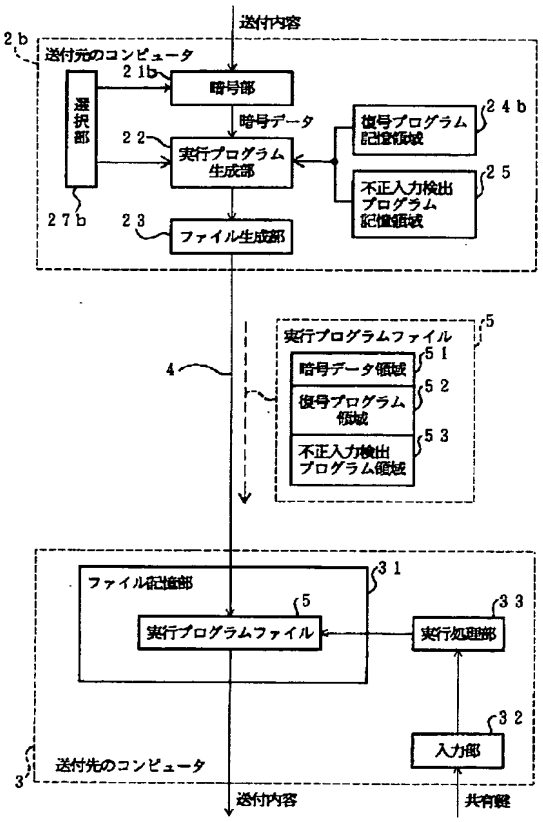
【図５】


1a
送付内容
2a
送付元のコンピュータ
21
暗号部
暗号データ
22a
実行プログラム生成部
23
ファイル生成部
24
復号プログラム記憶領域
25
不正入力検出プログラム記憶領域
26a
認証プログラム記憶領域
4
5a
実行プログラムファイル
51
暗号データ領域
52
復号プログラム領域
53
不正入力検出プログラム領域
54a
認証プログラム領域
31
ファイル記憶部
5a
実行プログラムファイル
33
実行処理部
32
入力部
3
送付先のコンピュータ
送付内容
共有鍵、パスワード

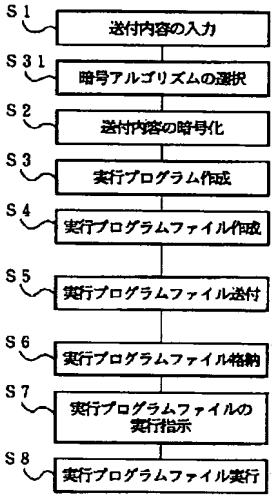
【図７】


スタート
S21
パスワード要求
S22
パスワード入力
S23
実行者の認証
?
失敗
成功
S11
共有鍵要求
S12
共有鍵入力
S13
正規の共有鍵
?
NO
YES
S14
暗号データの復号
S15
所定の回数超過
?
NO
YES
S16
実行プログラムファイル変更
エンド

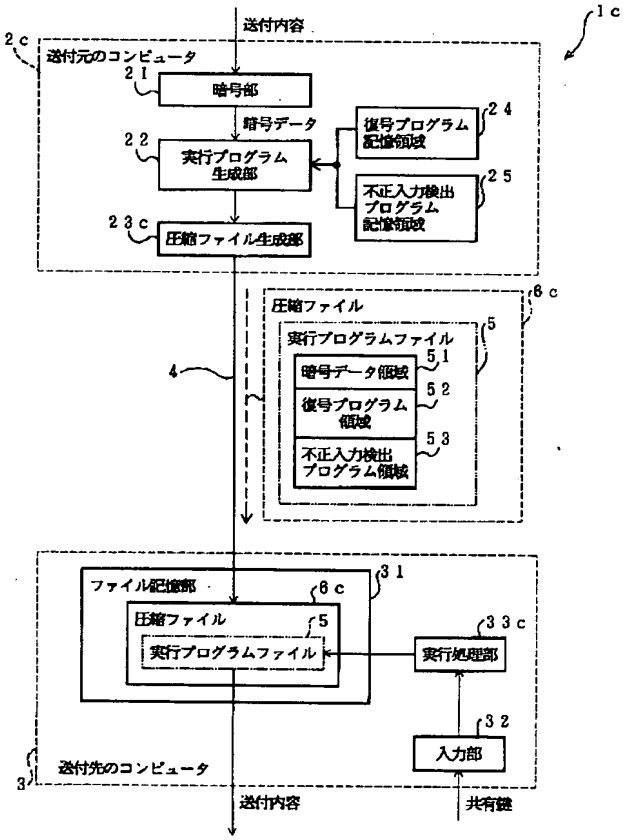
【図８】


送付内容
2b
送付元のコンピュータ
21b
暗号部
選択部
暗号データ
22
実行プログラム生成部
24b
復号プログラム記憶領域
25
不正入力検出プログラム記憶領域
27b
23
ファイル生成部
4
実行プログラムファイル
5
暗号データ領域
51
復号プログラム領域
52
不正入力検出プログラム領域
53
ファイル記憶部
31
実行プログラムファイル
5
実行処理部
33
入力部
32
3
送付先のコンピュータ
送付内容
共有鍵

【図９】


1b
S1
送付内容の入力
S31
暗号アルゴリズムの選択
S2
送付内容の暗号化
S3
実行プログラム作成
S4
実行プログラムファイル作成
S5
実行プログラムファイル送付
S6
実行プログラムファイル格納
S7
実行プログラムファイルの実行指示
S8
実行プログラムファイル実行

【図１０】


1c
送付内容
2c
送付元のコンピュータ
21
暗号部
暗号データ
22
実行プログラム生成部
24
復号プログラム記憶領域
25
不正入力検出プログラム記憶領域
23c
圧縮ファイル生成部
6c
圧縮ファイル
4
実行プログラムファイル
5
暗号データ領域
51
復号プログラム領域
52
不正入力検出プログラム領域
53
ファイル記憶部
31
圧縮ファイル
6c
5
実行プログラムファイル
33c
実行処理部
32
入力部
3
送付先のコンピュータ
送付内容
共有鍵